UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/594,106	07/24/2007	Fabien Thomas	CU-5118 BWH	8912

26530 7590 12/27/2007
LADAS & PARRY LLP
224 SOUTH MICHIGAN AVENUE
SUITE 1600
CHICAGO, IL 60604

EXAMINER	
TABOR, AMARE F	
ART UNIT	PAPER NUMBER
2139	
MAIL DATE	DELIVERY MODE
12/27/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/594,106	**Applicant(s)** THOMAS ET AL.	
	Examiner Amare Tabor	**Art Unit** 2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 April 2007*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *12/18/2006*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-12 are examined.

Specification

2. The disclosure is objected to because of the following informalities:

a. <u>Arrangement of the Specification</u>

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT.
(e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC.
(f) BACKGROUND OF THE INVENTION.
(1) Field of the Invention.
(2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(g) BRIEF SUMMARY OF THE INVENTION.
(h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(i) DETAILED DESCRIPTION OF THE INVENTION.
(j) CLAIM OR CLAIMS (commencing on a separate sheet).
(k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

b. **Abstract**

The abstract of the disclosure is objected to because the following sentences should be deleted: the title "*INVENTION PATENT*", "*ASQ V.2, 3 RUE ARCHIMEDE, 59650 VILLENEUVE, D'ASCQ*" and "*Figure 2.*"

c. **Claims**

In the claims the words "recognised", "authorisation" and "analysed" should be rewritten as "recognized", "authorization" and "analyzed" respectively.

Appropriate correction is required. See MPEP § 608.01(b).

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-12 are rejected under 35 U.S.C. 102(a) as being anticipated by "NETASQ IPS-Firewalls. ASQ: Real-Time Intrusion Prevention" (referred as "***ASQ V.2***" hereinafter) (AUTHOR: UNKNOWN; PUBLISHED: 2003).

As per Claim 1, ASQ V.2 teaches,

A method for the detection and prevention of intrusions into a computer network with a firewall, the method comprising (see *page 1*):

detecting the connections at a central point and before each branch of said network (see *ASQ and IPS* in the middle picture of *page 3*),

selective filtering of the said connections, where said selective filtering stage includes firstly a stage for automatic recognition of the accessing protocol, independently of the communication port used by the said protocol, and secondly, after said accessing protocol has been recognized automatically, a stage for verifying the conformity of each communication flowing in a given connection to the said protocol (see *Analysis of Application Protocols (ASQ plug-ins) in pages 5-7*),

to deliver a dynamic authorization for communications resulting from normal operation of the protocol (see *picture in page 1*; *Dynamic Filtering*; and *section Filtering (ASQ Dynamic Filtering)* in page 4) and to deliver a dynamic rejection for communications resulting from abnormal operation of the protocol (see *picture in page 1*; *Dynamic Filtering*; and *section Filtering (ASQ Dynamic Filtering)*,

wherein said check on conformity is performed layer by layer, by successive protocol analysis of each part of the data packet flowing in the connection corresponding to a given protocol, from the lowest protocol to the highest protocol (see *Principles of Packet Handling* in *page 3*),

and wherein, since each main connection enabled is able to induce one or more secondary connections, said check on conformity detects the data necessary for opening said secondary connections and attaches said secondary connections to the authorization for connection of said main connection (see *Protocol Analysis, Fragment Analysis, Global Context Analysis and Filtering* in *page 4*; and *ASQ strengths* in *page 9*).

As per Claim 2, ASQ V.2 teaches,

A method according to claim 1, wherein, as long as the accessing protocol of a connection is not recognized, the data are accepted but not transmitted (see *section Principles of Packet Handling and ASQ's strengths* in *page 3 & 9*).

As per Claim 3-4, ASQ V.2 teaches,

A method according to claim 2, wherein, if the number of data packets accepted but not transmitted exceeds a certain threshold, or if the data are accepted but not transmitted for a time exceeding a certain threshold, then the connection is considered not to have been analyzed; and wherein if the data are accepted but not transmitted for a time exceeding a certain threshold, then the connection is considered not to have been analyzed (see *section Real-time Monitoring and Historical Logging and ASQ's strengths* in *pages 8-9*).

As per Claim 5, ASQ V.2 teaches,

A method according to claim 2, wherein, when the accessing protocol of a connection is not automatically recognized, said step of checking on conformity of each communication flowing in a given connection to said protocol is replaced by a step of generic checking of coherence of data packets (see *section Analysis of Application Protocols (ASQ plug-ins)* from *page 5 to 9*).

As per Claim 6, ASQ V.2 teaches,

A device for the detection and prevention of intrusions into a computer network, comprising (see *section ASQ: Real-Time Intrusion Prevention* in *page 1*):

a firewall (see *page 1*), a resource for preventing intrusions by detection of the connections (*ASQ engine*), directly incorporated into said firewall at a central point and before each branch of said network, where said resource for the prevention of intrusions includes a resource for selective filtering of said connections by automatic recognition of the accessing protocol, independently of the communication port used by said protocol (see *section An integrated Firewall / IPS Solution* in *page 1*), wherein said selective filtering resource includes at least one independent module for the analysis of at least one given communication protocol, and at least one of the independent modules includes:

i. unit for the automatic recognition of a given communication protocol (see *section Protocol Analysis* in *page 4*),

ii. unit for verifying the conformity of the communication flowing in a given connection to the said protocol (see *picture in page 1*; *Dynamic Filtering*; and *section Filtering (ASQ Dynamic Filtering)* in page 4),

iii. means for delivering a dynamic authorization for communications resulting from normal operation of the protocol, and delivering a dynamic rejection for communications resulting from abnormal operation of the protocol (see *picture* in *page 1*; *Real Time Intrusion Prevention*), and

iv. means of transmission of a part of a data packet to an independent analysis module of a hierarchically higher protocol (see *section Principle of Packet Handling* in page 2).

As per Claim 7, ASQ V.2 teaches,

A device according to claim 6, wherein, in addition to the independent module or modules for the analysis of a given communication protocol, the device includes an independent generic module which attaches itself to the connections for which the protocol has been recognized by none of the other said independent modules (see *section Analysis of Application Protocols (ASQ plug-ins);* and *picture* in *page 3 - IPS-Plugin*).

As per Claim 8, ASQ V.2 teaches,

A device according to claim 6, wherein the device includes an interface for entry, by a user, of the criteria that determine the filtering policy (see *Interfaces* in *pages 5 & 6*).

As per Claim 9-10, ASQ V.2 teaches,

A device according to claim 8, wherein, said interface receives the criteria specified in natural language by the user; and wherein said criteria specified in natural language include at least one protocol name (see *[HTTP], [FTP], [DNS], [eDonkey], [H323], [RIP] and [Generic]* n pages 6 and 7).

As per Claim 11, ASQ V.2 teaches,

A device according to claim 8, wherein said interface allows the activation or deactivation of each of said independent modules (see *Protocol Analysis, Fragment Analysis, Global Context Analysis and Filtering* in *page 4*; and *ASQ strengths* in *page 9*).

As per Claim 12, ASQ V.2 teaches,

A device according to claim 6, wherein the device includes a resource for statistical processing of the connection data, and a resource for storage of said connection data and processed data (see *section Real-time Monitoring and Historical Logging* in *page 8*).

Claims 1-12 are rejected under 35 U.S.C. 102(e) as being anticipated by "*YADAV*" (US 7,174,566).

As per Claim 1, YADAV teaches,

A method for the detection and prevention of intrusions into a computer network with a firewall (see *abstract; and col. 1, lines 6-8*), the method comprising:

detecting the connections at a central point and before each branch of said network (see *MONITOR INBOUND TRAFFIC AND TRAFFICT CORRESPONDING TO A WATCH LIST 105 IN Fig. 1*),

selective filtering of the said connections (see *col.7, line 19 to col. 8, line 15*), where said selective filtering stage includes firstly a stage for automatic recognition of the accessing protocol, independently of the communication port used by the said protocol (see *Fig. 3*),

and secondly, after said accessing protocol has been recognized automatically, a stage for verifying the conformity of each communication flowing in a given connection to the said protocol (see *COMPARE REQUEST WITH NETWORK POLICY 320 and NETWORK POLICY SATISFIED? 325 IN Fig. 3*),

to deliver a dynamic authorization for communications resulting from normal operation of the protocol (see *NOTIFY NETWORK TRAFFIC ENFORCER OF OPEN CHANNEL 330 IN Fig.* 3) and to deliver a dynamic rejection for communications resulting from abnormal operation of the protocol (see *NOTIFY INTRUSION DETECTOR OF UNAUTHORIZED REQUEST 335 IN Fig. 3*),

wherein said check on conformity is performed layer by layer, by successive protocol analysis of each part of the data packet flowing in the connection corresponding to a given protocol, from the lowest protocol to the highest protocol (see *LOAD APPLICATION-SPECIFIC NETWORK POLICY 310 in Fig. 3*),

and wherein, since each main connection enabled is able to induce one or more secondary connections, said check on conformity detects the data necessary for opening said secondary connections and attaches said secondary connections to the authorization for connection of said main connection (see *APPLICATION AND RULE ENFORCER COMPONENT ARE INVOKED 300 and IDENTITY INVOKED APPLICATION (APPLY HASH FUNCTION AND CHECK RESULT) 305 in Fig. 3*).

As per Claim 2, YADAV teaches,

A method according to claim 1, wherein, as long as the accessing protocol of a connection is not recognized, the data are accepted but not transmitted *(see SEND UNAUTHORIZED COMMUNICATION TO INTRUSION DETECTOR and BLOCK UNAUTHORIZED COMMUNICATION in Fig. 4; and fro example, col. 8, lines 16-33*).

As per Claim 3-4, YADAV teaches,

A method according to claim 2, wherein, if the number of data packets accepted but not transmitted exceeds a certain threshold (see *COMPARE WITH CONFIGURABLE THRESHOLD 555 in Fig. 5A*), or if the data are accepted but not transmitted for a time exceeding a certain threshold (see *Time Elapsed in Fig. 5B*), then the connection is considered not to have been analyzed; and wherein if the data are accepted but not transmitted for a time exceeding a certain threshold, then the connection is considered not to have been analyzed (see *Fig. 5B; and for example, col. 9, lines 4-52*).

As per Claim 5, YADAV teaches,

A method according to claim 2, wherein, when the accessing protocol of a connection is not automatically recognized, said step of checking on conformity of each communication flowing in a given connection to said protocol is replaced by a step of generic checking of coherence of data packets (see *Fig. 5A; and for example, col. 8, line 34 to col. 9, line 3*).

As per Claim 6, YADAV teaches,

A device for the detection and prevention of intrusions into a computer network (see *abstract; and col. 1, lines 6-8; Fig. 2A-B and 6*), comprising:

a firewall, a resource for preventing intrusions by detection of the connections, directly incorporated into said firewall at a central point and before each branch of said network (see *Intrusion DetectiOn System 230, 234, 236 and 280 in Fig. 2A-B*) where said resource for the prevention of intrusions includes a resource for selective filtering of said connections by automatic recognition of the accessing protocol, independently of the communication port used by said protocol, wherein said selective filtering resource includes at least one independent module for the analysis of at least one given communication protocol (see *224,... and 236,... in Fig. 2A*) , and at least one of the independent modules includes (see *col. 4, line 59 to col. 7, line 18*):

i. unit for the automatic recognition of a given communication protocol (see *NETWORK TRAFFIC ENFORCER 282 in Fig. 2A*),

ii. unit for verifying the conformity of the communication flowing in a given connection to the said protocol (see *INTRUSION DETECTOR 280 in Fig. 2A-B*),

iii. means for delivering a dynamic authorization for communications resulting from normal operation of the protocol, and delivering a dynamic rejection for communications resulting from abnormal operation of the protocol (see *APPLICATION RULE ENFORCER 284 in Fig. 3*), and

iv. means of transmission of a part of a data packet to an independent analysis module of a hierarchically higher protocol (see *Network Transport Layer 260 in Fig. 2A-B*).

As per Claim 7, YADAV teaches,

A device according to claim 6, wherein, in addition to the independent module or modules for the analysis of a given communication protocol, the device includes an independent generic module which attaches itself to the connections for which the protocol has been recognized by none of the other said independent modules (see *APPLICATION AND RULE ENFORCER COMPONENT ARE INVOKED 300 and IDENTITY INVOKED APPLICATION (APPLY HASH FUNCTION AND CHECK RESULT) 305 in Fig. 3; and for example, col. 7, line 19 to col. 8, line 15*).

As per Claim 8, YADAV teaches,

A device according to claim 6, wherein the device includes an interface for entry, by a user, of the criteria that determine the filtering policy (see *Security Operation Center 242 & 292 in Fig. 2A-B; and for example, col. 5, lines 33-41*).

As per Claim 9-10, YADAV teaches,

A device according to claim 8, wherein, said interface receives the criteria specified in natural language by the user (see *Response Needed? 515 in Fig. 5A*; *and for example, col. 5, lines 33-41 and col. 6, lines 17-24*), wherein said criteria specified in natural language include at least one protocol name (see *col. 1, lines 6-67*).

As per Claim 11, YADAV teaches,

A device according to claim 8, wherein said interface allows the activation or deactivation of each of said independent modules (see *Fig. 1, 3 and 5A-B; where independent modules analysis is disclosed*).

As per Claim 12, YADAV teaches,

A device according to claim 6, wherein the device includes a resource for statistical processing of the connection data, and a resource for storage of said connection data and processed data (see *LOG NETWORK ACTIVITY 525, EXAMINE COMMUNICATION(S) FOR INTUSION PRELUDE PATTERNS 505, LOG NETWORK ACTIVITY FOR LATER ANALYSIS 545 & 585 IN Fig. 5A-B*).

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Amare Tabor whose telephone number is (571) 270-3155. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Amare Tabor
AU 2139

12/18/2007
SYED A. ZIA
PRIMARY EXAMINER